

Cooperative Secret Communication with Artificial Noise in Symmetric Interference Channel

Jingge Zhu, Jianhua Mo and Meixia Tao, *Member, IEEE*

Abstract—We consider the symmetric Gaussian interference channel where two users try to enhance their secrecy rates in a cooperative manner. Artificial noise is introduced along with useful information. We derive the power control and artificial noise parameter for two kinds of optimal points, max-min point and single user point. It is shown that there exists a critical value P_c of the power constraint, below which the max-min point is an optimal point on the secrecy rate region, and above which time-sharing between single user points achieves larger secrecy rate pairs. It is also shown that artificial noise can help to enlarge the secrecy rate region, in particular on the single user point.

Index Terms—Gaussian interference channel, secrecy capacity, power control.

I. INTRODUCTION

The problem of secret communication is considered in the seminal paper of Wyner [1]. It is shown that perfect secrecy can be achieved without any key, provided that the receiver has a better channel than the eavesdropper. Recently, the secret communication in wireless networks has been intensively studied for various scenarios. Broadcast channel with confidential message is considered in [2] whereas multiple-access channels with secrecy constraint is studied in [3] and [4]. The secrecy rate region of Gaussian interference channel with an external eavesdropper is investigated in [5].

In this work, we consider the secret communication in a two-user symmetric interference channel as shown in Fig. 1 where each receiver has to decode its own message while eavesdropping on the other's message. It is first pointed out in [6] that by introducing artificial noise in the transmission along with the useful information, the secrecy rate region can be enlarged as the artificial noise causes additional interference to the eavesdropper. The key idea in our work is that although the two users in this system do not trust each other because both can potentially eavesdrop on the other's message, nevertheless, they can enhance their secrecy rates in a cooperative manner. It is called *semi-secret* in [7] as the achieved secret communication depends on trusting other transmitters.

We derive the optimal power control and artificial noise parameter for two different points on the secrecy rate region, namely, max-min point and single user point. We show that depending on the relationship of power constraint and channel conditions, both points can potentially achieve optimal secrecy

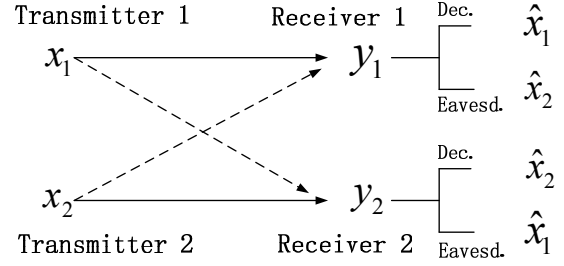


Fig. 1. Interference channel with confidential messages.

rate pairs. A criterion is given explicitly. We also show that while it is not helpful in improving the max-min point, artificial noise can enlarge the secrecy rate on single user point.

Notation $(\cdot)^T$ denotes transpose. $\mathbb{E}\{x\}$ stands for expectation of random variable x . The function $\log(\cdot)$ is taken to the base 2.

II. SYMMETRIC INTERFERENCE CHANNEL WITH ARTIFICIAL NOISE

The symmetric interference channel can be modeled as

$$y_1 = \sqrt{a}x_1 + \sqrt{a_c}x_2 + n_1 \quad (1a)$$

$$y_2 = \sqrt{a_c}x_1 + \sqrt{a}x_2 + n_2 \quad (1b)$$

where a and a_c are the gains for the direct channels and cross channels, respectively, the transmitted signal x_i , for $i = 1, 2$, is subject to the peak power constraint $\mathbb{E}\{|x_i|^2\} = p_i \leq P$, and n_i is the additive white Gaussian noise with zero mean and variance N . The transmitted signal x_i is composed of message s_i and artificial noise z_i , i.e. $x_i = s_i + z_i$. Here z_i is chosen to be Gaussian hence cannot be decoded by any receiver. We split the transmission power as $\mathbb{E}\{s_i^2\} = (1 - \lambda_i)p_i$ and $\mathbb{E}\{z_i^2\} = \lambda_i p_i$, with parameter $\lambda_i \in [0, 1]$.

The formal definition of secrecy rate for the interference channel can be found in [8], which considers the case where only one user sends artificial noise. We generalize their work to allow both users to use artificial noise and define the achievable secrecy rate region under our setting as follows.

Let (R_1, R_2) denote a rate pair satisfying (2). Then the secrecy rate region is the union of all possible rate pairs (R_1, R_2) for transmission power $0 \leq p_i \leq P$ and power splitting parameter $0 \leq \lambda_i \leq 1$, $i = 1, 2$.

The achievability of the secrecy rate region defined above can be justified using the similar stochastic encoding argument in [8]. If time-sharing between transmission strategies is allowed, the convex hull of the above rate region can also be achieved. We can interpret the constraint (2) as follows:

Manuscript received 28-Jun-2010. The associate editor coordinating the review of this letter and approving it for publication was J. Jalden.

The authors are with Dept. of Electronic Engineering, Shanghai Jiao Tong University, P. R. China. Emails: {zhujingge, mjh, mxtao}@sjtu.edu.cn.

This work was supported in part by the NSF of China under grant 60902019 and Shanghai Pujiang Talent Program under grant 09PJ1406000.

$$0 \leq R_1 \leq R_1^s := \log \left(1 + \frac{a(1-\lambda_1)p_1}{N + a_c p_2 + a \lambda_1 p_1} \right) - \log \left(1 + \frac{a_c(1-\lambda_1)p_1}{N + a_c \lambda_1 p_1 + a \lambda_2 p_2} \right) \quad (2a)$$

$$0 \leq R_2 \leq R_2^s := \log \left(1 + \frac{a(1-\lambda_2)p_2}{N + a_c p_1 + a \lambda_2 p_2} \right) - \log \left(1 + \frac{a_c(1-\lambda_2)p_2}{N + a_c \lambda_2 p_2 + a \lambda_1 p_1} \right) \quad (2b)$$

In any working system, the receiver can always decode its own message successfully by considering interferences as pure noise, then it subtracts the already decoded message and try to decode the message from the other transmitter. The difference on the right-hand side of each of the two constraints is the maximum amount of information one can hide from the other, from an information theoretic point of view.

Note that nonnegative secrecy rate only exists when the direct channel is stronger than the cross channel. This can be verified directly with the expression of R_1^s or R_2^s . So we only consider the case where $a > a_c$ hereafter.

III. MAIN RESULTS

In this section, we present the main results on the optimal power allocation $\{p_i, \lambda_i\}_{i=1}^2$ on two points of the secrecy rate region, namely, max-min point and single user point.

A. Max-min Point

We first define an optimal point in the following sense:

$$R_{min}^* := \max_{\{\lambda_i, p_i\}} \min\{R_1, R_2\}.$$

Note that since the second inequality in (2a) and (2b) can be tight simultaneously, the above definition is equivalent to $R_{min}^* := \max_{\{\lambda_i, p_i\}} \min\{R_1^s, R_2^s\}$.

Proposition 1: For interference channel (1), $R_{min}^* = \log \left(\frac{(a+a_c)^2}{4aa_c} \right)$ with $\lambda_1^* = \lambda_2^* = \lambda^*$, where λ^* can be chosen arbitrarily from the interval $[0, \frac{a_c}{a} - \frac{N(a-a_c)}{Pa(a+a_c)}]$, and $p_1^* = p_2^* = p^* = \frac{N(a-a_c)}{(a+a_c)(a_c-a\lambda^*)}$. Among the maximizing points, $\lambda^* = 0$ yields the minimum transmission power $p_{min}^* = \frac{N(a-a_c)}{a_c(a+a_c)}$. If the power constraint $P < p_{min}^*$, the maximizing points are $\lambda^* = 0$ and $p^* = P$.

Proof: It is intuitive to see that in order to achieve the point R_{min}^* , we need $p_1 = p_2 = p$ and $\lambda_1 = \lambda_2 = \lambda$ because of the competitive nature of the two users. This will be justified at the end of the proof. We will now maximize

$$R_1^s = R_2^s = R^s = \log \frac{(N + a_c p + ap)(N + a_c \lambda p + a \lambda p)}{(N + a_c p + a \lambda p)(N + a \lambda p + a_c p)}.$$

The maximum value of R^s should satisfy:

$$\frac{\partial R^s}{\partial p} = 0, \quad \frac{\partial R^s}{\partial \lambda} = 0 \quad (3)$$

It is found that for arbitrary λ , choosing

$$p(\lambda) = \frac{N(a-a_c)}{(a+a_c)(a_c-a\lambda)} \quad (4)$$

always forms a solution to (3). It can also be shown that the second-order derivatives of R^s are negative at these points, i.e., they are all maximizing points of the function. Taking the

constraints $\lambda \in [0, 1]$ and $p(\lambda) \in [0, P]$ into consideration, we see that the valid value of λ^* should be in the interval $[0, \frac{a_c}{a} - \frac{N(a-a_c)}{Pa(a+a_c)}]$, and the optimal p^* is obtained by substituting λ^* into (4). Note that the possible maximizing points on the boundary ($\lambda = 0$ for example, which cannot be found by solving the equations (3)) are also included in the solution.

The minimum required transmission power maintaining the secrecy rate R_{min}^* is $p_{min}^* = \frac{N(a-a_c)}{a_c(a+a_c)}$ by choosing $\lambda^* = 0$. In the case where $P < p_{min}^*$, there is no solution to (3) satisfying the constraint $\lambda \in [0, 1]$, and the R_{min}^* is achieved by $\lambda^* = 0$ and $p^* = P$ since R^s is now increasing with p and decreasing with λ .

We now justify that the same transmission power p and power splitting parameter λ are indeed required to achieve R_{min}^* . Define $\mathbf{A} = \nabla R_1^s(\lambda^*, p^*) \nabla R_2^{sT}(\lambda^*, p^*)$, where $\nabla R_i^s = [\partial R_i^s / \partial p_1, \partial R_i^s / \partial p_2, \partial R_i^s / \partial \lambda_1, \partial R_i^s / \partial \lambda_2]^T$ is the gradient of R_i^s , and $\nabla R_i^s(\lambda^*, p^*)$ means ∇R_i^s evaluated at the point $\lambda_1 = \lambda_2 = \lambda^*, p_1 = p_2 = p^*$. It is clear that \mathbf{A} has only one eigenvalue which is equal to its trace, given by

$$tr(\mathbf{A}) = \frac{\partial R_1^s}{\partial p_1} \frac{\partial R_2^s}{\partial p_1} + \frac{\partial R_1^s}{\partial p_2} \frac{\partial R_2^s}{\partial p_2} + \frac{\partial R_1^s}{\partial \lambda_1} \frac{\partial R_2^s}{\partial \lambda_1} + \frac{\partial R_1^s}{\partial \lambda_2} \frac{\partial R_2^s}{\partial \lambda_2}.$$

Straightforward calculation shows that $\frac{\partial R_i^s}{\partial p_j}(\lambda^*, p^*)$ is negative for $i \neq j$ and positive for $i = j$. Also, $\frac{\partial R_i^s}{\partial \lambda_j}(\lambda^*, p^*)$ is positive for $i \neq j$ and negative for $i = j$. So $tr(\mathbf{A})$ is always negative. Therefore, \mathbf{A} is negative definite hence $\mathbf{d}^T \mathbf{A} \mathbf{d} < 0$ for any $\mathbf{d} \neq \mathbf{0}$. Note that $\mathbf{d}^T \mathbf{A} \mathbf{d}$ can also be rewritten as

$$\nabla R_1^{sT}(\lambda^*, p^*) \mathbf{d} \cdot \nabla R_2^{sT}(\lambda^*, p^*) \mathbf{d} < 0. \quad (5)$$

Inequality (5) means that any deviation from the optimal points will decrease the value of either R_1^s or R_2^s , thereby, the minimum of the two becomes smaller. In other words, the deviated point cannot be a max-min point. Thus, our choices of p and λ are validated and the proposition is proved. ■

B. Single User Point

We now investigate another point, called *single user point*, on which one user tries to maximize its own secrecy rate with the help of the other user, i.e. $R_{su,i}^* = \max R_i^s$. It is clear that due to the symmetry, we have $R_{su,1}^* = R_{su,2}^* = R_{su}^*$. We will show that through this kind of cooperation, one user obtains an appreciably large secrecy rate while the secrecy rate of the other is zero. In addition, we also find that through time-sharing, we can achieve larger rate pairs than the max-min point when P is greater than a critical value.

Proposition 2: The single user point R_{su}^* is obtained with $(\lambda_1^* = 0, \lambda_2^* = 1, p_1^* = P, p_2^* = \frac{\Delta-N}{a+a_c})$ or $(\lambda_1^* = 1, \lambda_2^* = 0,$

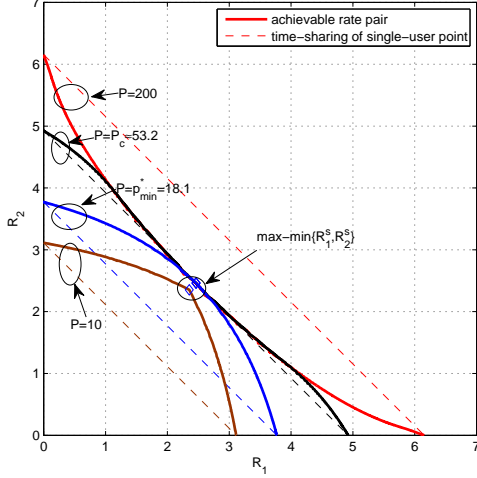


Fig. 2. Achievable secrecy rate region for different power constraint at $a = 1$, $a_c = 0.05$ and $N = 1$. The critical power $P_c \approx 53.2$ and $p_{min}^* \approx 18.1$.

$p_1^* = \frac{\Delta - N}{a + a_c}$, $p_2^* = P$) and it is given by

$$R_{su}^* = \max R_1^s = \max R_2^s = \log \left(\frac{(aN + a_c\Delta)(a_cN + a\Delta) + a(a + a_c)(a_cN + a\Delta)P}{(aN + a_c\Delta)(a_cN + a\Delta) + a_c(a + a_c)(aN + a_c\Delta)P} \right) \quad (6)$$

with $\Delta = \sqrt{N^2 + (a + a_c)NP}$.

Proof: Without loss of generality, we analyze the single user point for user 1 only. From (2a), R_1^s is decreasing with λ_1 and increasing with both λ_2 and p_1 . Hence, to maximize R_1^s we should have $\lambda_1^* = 0$, $\lambda_2^* = 1$ and $p_1 = P$. Substituting them into R_1^s and solving the equation $\frac{\partial R_1^s}{\partial p_2} = 0$ for p_2 , we find $p_2^* = \frac{\Delta - N}{a + a_c} < \frac{P}{2}$. It can again be justified with the second-order derivative that it is indeed the maximized point. ■

We now compare the secrecy rate pairs achieved by max-min point and single user point. At max-min point, each user gets the same secrecy rate R_{min}^* , given in Proposition 1. By equal time-sharing between the two single user points, each user gets the same secrecy rate $R_{su}^*/2$, where R_{su}^* is given in Proposition 2.

Proposition 3: When the power constraint P is larger than the critical power $P_c = \frac{N(a - a_c)(a^2 + a_c^2 + 6aa_c)}{(a_c^2 + 3aa_c)^2}$, equal time-sharing between single user points achieves larger rates than the max-min point, otherwise, the max-min point achieves larger rates.

Proof: This proposition can be easily proved by solving $R_{su}^* = 2R_{min}^*$ and using the monotonicity of R_{su}^* . ■

IV. NUMERICAL EXAMPLES AND DISCUSSIONS

Fig. 2 demonstrates some numerical results on the achievable secrecy rate region for different power constraints with fixed channel condition. When $P = P_c$, the max-min point (diamond in the figure) is the same point obtained by equal time-sharing of two single user points, otherwise there are significant gaps between the achievable rates of two methods. When $P \geq p_{min}^*$, the max-min points of different P coincide. These results verify our analytical findings in Proposition 1.

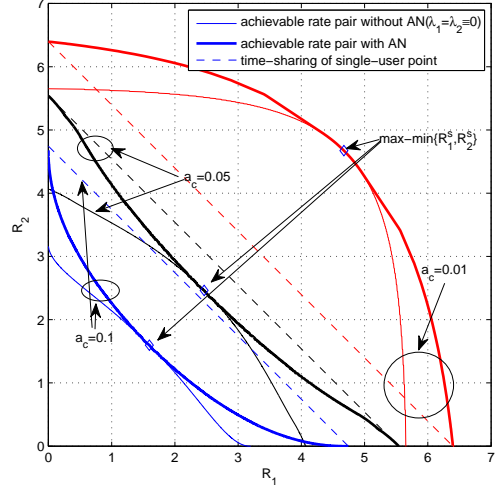


Fig. 3. Achievable secrecy rate region for different channel conditions at $a = 1$, $N = 1$, $P = 100$.

Fig. 3 shows the benefit of the artificial noise (AN). The secrecy rates with and without artificial noise ($\lambda_1 = \lambda_2 \equiv 0$) are plotted for fixed P but different channels. We observe that the rate region with artificial noise is always larger than that without artificial noise, in particular, artificial noise increases the secrecy rate achieved on single user point. For $a_c = 0.01$, the point R_{min}^* is the optimal point and is superior than points achieved by time-sharing. For larger a_c , the optimal points are obtained by time-sharing.

The above results show that the secrecy rate region in cooperative symmetric interference channel with artificial noise behaves significantly different from the classical capacity in symmetric interference channel ([9]). When classical capacity is concerned, the max-min point is always attained when the sum rate $R_1 + R_2$ is also maximized. However, for secrecy capacity, the point $\max(R_1^s + R_2^s)$ does not necessarily coincide with R_{min}^* all the time.

REFERENCES

- [1] A. D. Wyner, "The wire-tap channel," *Bell. Syst. Tech. J.*, vol. 54, no. 8, 1975.
- [2] Y. Liang and H. V. Poor, "Secure communication over fading channels," *IEEE Trans. on Infor. Theory*, vol. 52, no. 6, pp. 2470–2492, June 2008.
- [3] E. Tekin and A. Yener, "The general Gaussian multiple access and two-way wire-tap channels: Achievable rates and cooperative jamming," *IEEE Trans. on Infor. Theory*, vol. 54, no. 6, pp. 2735–2751, June 2008.
- [4] Y. Liang and H. V. Poor, "Multiple access channels with confidential messages," *IEEE Trans. on Infor. Theory*, vol. 54, no. 3, pp. 976–1002, March 2008.
- [5] O. Koyluoglu and H. Gamal, "On the secrecy rate region for the interference channel," in *Proc. IEEE PIMRC*, 2008.
- [6] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Comm.*, vol. 7, no. 6, Jun, 2008.
- [7] R. D. Yates, D. Tse, and Z. Li, "Secret communication on interference channels," in *Proc. IEEE Int. Symp. Information Theory*, July 2008.
- [8] R. Liu, I. Maric, P. Spasojevic, and R. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate region," *IEEE Trans. on Infor. Theory*, vol. 54, no. 6, Jun. 2008.
- [9] R. Etik, D. Tse, and H. Wang, "Gaussian interference channel capacity to within one bit," *IEEE Trans. on Infor. Theory*, vol. 54, no. 12, Dec. 2008.